UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,865	11/09/2001	Jesse R. Walker	042390.P12264	6559

7590 08/18/2005

R. Alan Burnett
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 08/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/007,865	WALKER, JESSE R.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 8 recites the limitation "the common cryptographic key" in line 1 where a common cryptographic key has not previously been introduced. Thus, there is insufficient antecedent basis for this limitation in the claim. In order to further treat this claim on its merits, it is presumed that applicants intended to refer to the common encryption key that was previously introduced in the parent claim.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 3-4, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and further in view of Lynn et al., US Patent No. 5,345,508.

As per claim 1:

Hellman et al. substantially teach a method for bootstrapping a secure communications channel between devices, comprising: generating a key via a first device and establishing a short range communication channel between the first device and a second device (col. 4, lines 1-17); sending a copy of the key from the first device to the second device via the short range communication channel to produce a shared key that is shared by both the first and second devices (col. 4, lines 44-68); establishing a secure communication channel between the first and second devices using an encrypted communication protocol that implements an encryption scheme based on a common encryption key derived from the shared key (col. 5, lines 1-3).

Not explicitly disclose is said secure communication channel being separate and apart from the short range communication channel. However, Lynn et al. teach that the key should be generated and communicated through a channel separate from the cipher text. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. for the secure communication channel to be separate from the short range communication channel. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lynn et al. in col. 4, lines 58-62.

As per claim 3:

Hellman et al. and Lynn et al. substantially teach the method of claim 1. Not explicitly disclosed is the method further comprising disabling the short range communication channel after the copy of the key has been sent from the first device to the second device. However, Lynn et al. teach that the short range communication is only used for communicating the key and that it is no longer used for the remainder of the communication. Therefore, it would have been

obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to disable the short range communication channel after the copy of the key has been transmitted to the second device from the first device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lynn et al. in col. 4, lines 39-62.

As per claim 4:

Hellman et al. and Lynn et al. substantially teach the method of claim 1. Furthermore, Hellman et al. teach the method wherein the shared key comprises a cryptographically secure pseudo-random number (col. 4, lines 1-11).

As per claim 8:

Hellman et al. and Lynn et al. substantially teach the method of claim 1. Furthermore, Hellman et al. teach the method wherein the common encryption key is the shared key (col. 4, line 60 – col. 5, line 3).

III. Claims 2, 5, and 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and Lynn et al., US Patent No. 5,345,508 as applied to claim 1 above, and further in view of Clapp, US Patent No. 5,987,131.

As per claim 2:

Hellman et al. and Lynn et al. substantially teach the method of claim 1. Not explicitly disclosed is the method further comprising sending identity information used to identify the first device from the first device to the second device, wherein the identity information is used to establish the secure communication channel. However, Clapp teaches that a first device sends a certificate to a second device in order for the second device to verify the first device's identity

before establishing a secure communication channel. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to send identity information in order to establish the secure communication channel. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Clapp in col. 5, lines 14-35.

As per claim 5:

Hellman et al. and Lynn et al. substantially teach the method of claim 1. Not explicitly disclosed is the method wherein each of the first and second devices include an authenticated key agreement algorithm software component that is used to cooperatively generate the common encryption key. However, Clapp teaches that the two devices have a key agreement protocol. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. for the first and second devices to include an authenticated key agreement algorithm software component used to generate the common encryption key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Clapp in col. 4, line 65 – col. 5, line 4.

As per claim 9:

Hellman et al. and Lynn et al. substantially teach the method of claim 1. Not explicitly disclosed by Hellman et al. is the method further comprising performing a peer-to-peer authentication using symmetric authenticated key agreement algorithms running on both devices and the shared key. However, Clapp teaches that each device must authenticate the other

through the use of identity information, as well as a key agreement protocol. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to perform a peer-to-peer authentication using symmetric authenticated key agreement algorithms running on both devices and the shared key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Clapp in col. 4, line 65 – col. 5, line 35.

As per claim 10:

Hellman et al., Lynn et al., and Clapp substantially teach the method of claim 9. Furthermore, Clapp teaches the method wherein the peer-to-peer authentication is implemented by performing the operations of: storing credentials data including at least the shared key on both the first and second devices (col. 5, lines 5-35); generating a first random string with the first device and passing the first random string to the second device (col. 4, lines 9-18); generating a first digital signature corresponding to the first random string with the first device using an encryption key derived from the credentials data stored on the first device and a symmetric authenticated key agreement algorithm running on the first device (col. 5, lines 14-35); generating a second digital signature corresponding to the first random string with the second device using an encryption key derived from the credentials data stored on the second device and a symmetric authenticated key agreement algorithm running on the second device (col. 5, lines 53-64); comparing the first and second digital signatures to see if they match (col. 5, lines 14-35); and authenticating the second device with the first device if there is a match (col. 5, lines 36-

52).

As per claim 11:

Hellman et al., Lynn et al., and Clapp substantially teach the method of claim 10. Not explicitly disclosed is the method wherein the peer-to-peer authentication further comprises performing the operation of: generating a second random string with the second device and passing the second random string to the first device; generating a third digital signature corresponding to the second random string with the second device using an encryption key derived from the credentials data stored on the second device and a symmetric authenticated key agreement algorithm running on the second device; generating a fourth digital signature corresponding to the second random string with the first device using an encryption key derived from the credentials data stored on the first device and a symmetric authenticated key agreement algorithm running on the first device; comparing the third and fourth digital signatures to see if they match; and authenticating the first device with the second device if there is a match.

However, Clapp teaches verifying the identity of each of the devices using digital signatures of the devices for security purposes. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to create a third and fourth digital signature in order to double-check and put each of the devices through a more extensive verification process in order to more securely authenticate each of the devices to one another. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Clapp in col. 1, line 64 – col. 2, line 17 and col. 5, lines 5-64.

IV. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and Lynn et al., US Patent No. 5,345,508 as applied to claim 1 above, and further in view of Raspotnik, US Patent No. 5,832,090.

As per claim 6:

Hellman et al. and Lynn et al. substantially teach the method of claim 1. Not explicitly disclosed is the method wherein the short range communication channel comprises a transponder/transponder reader pair and wherein the transponder is operatively coupled to the first device and the transponder reader is operatively coupled to the second device. However, Raspotnik teaches using a transponder/transponder reader in order to generate a secret key via a communications link. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. for the short range communication channel to comprise a transponder/transponder reader pair coupled to the first and second devices. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Raspotnik in col. 2, lines 36-51.

As per claim 7:

Hellman et al., Lynn et al. and Raspotnik substantially teach the method of claim 6. Furthermore, Raspotnik teach the method wherein the transponder reader is coupled to an antenna that radiates radio frequency (RF) energy that is used to energize the transponder, further comprising waving the transponder in front of or placing the transponder in proximity to the transponder reader to energize the transponder and cause the transponder to transmit data

pertaining to the key to enable the data to be read by the transponder reader via the antenna (col. 2, lines 36-62).

V. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and further in view of Leibholz et al., US Patent No. 4,783,798.

As per claim 12:

Hellman et al. substantially teaches a method for bootstrapping a secure communications channel between devices, comprising: generating a key via a first device (col. 4, lines 1-17); storing the copy of the key in the second device to produce a shared key that is shared by both the first and second devices (col. 4, lines 44-68); establishing a secure communication channel between the first and second devices using an encrypted communication protocol that implements an encryption scheme based on a common encryption key derived from the shared key (col. 5, lines 1-3).

Not explicitly disclosed is activating a transponder reader in a second device and transmitting data corresponding to a copy of the key from a transponder operatively coupled to the first device to the transponder reader. However, Leibholz et al. teach different modes in which a transponder operates and receives data corresponding to a copy of a key sent from the first device. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to transmit data corresponding to a copy of the key from the first device's transponder after activating a transponder reader in the second device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Leibholz et al. in col. 3, lines 40-58 and col. 5, lines 13-23.

VI. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and Leibholz et al., US Patent No. 4,783,798 as applied to claim 12 above and further in view of Lynn et al., US Patent No. 5,345,508.

As per claim 13:

Hellman and Leibholz et al. substantially teach the method of claim 12. Not explicitly disclosed is the method further comprising disabling at least one of the transponder and transponder reader after the copy of the key has been sent from the first device to the second device. However, Lynn et al. teach that the short range communication is only used for communicating the key and that it is no longer used for the remainder of the communication. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to disable the short range communication channel after the copy of the key has been transmitted to the second device from the first device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Lynn et al. in col. 4, lines 39-62.

VII. Claims 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and Leibholz et al., US Patent No. 4,783,798 as applied to claim 12 above and further in view of Raspotnik, US Patent No. 5,832,090.

As per claim 14:

Hellman et al. and Leibholz et al. substantially teach the method of claim 12. Not explicitly disclosed is the method wherein the transponder reader is coupled to an antenna that radiates radio frequency (RF) energy that is used to energize the transponder, further comprising

waving the transponder in front of or placing the transponder in proximity to the transponder reader to energize the transponder and cause the transponder to transmit a signal containing the data corresponding to the copy of the key to enable the data to be read by the transponder reader via the antenna.

However, Raspotnik teaches that the transponder reader is coupled to an antenna that radiates radio frequency energy which energizes the transponder where the transponder is enabled to read the key data via the antenna. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. for the transponder reader is coupled to an antenna that radiates radio frequency (RF) energy that is used to energize the transponder, further comprising waving the transponder in front of or placing the transponder in proximity to the transponder reader to energize the transponder and cause the transponder to transmit a signal containing the data corresponding to the copy of the key to enable the data to be read by the transponder reader via the antenna. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Raspotnik in col. 2, lines 36-62.

As per claim 15:

Hellman et al., Leibholz et al., and Raspotnik substantially teach the method of claim 14. Furthermore, Raspotnik teaches the method wherein the transponder reader further transmits data via the antenna requesting the transponder to send data to the transponder reader and the transponder sends the data corresponding to the copy of the key in response to receiving the request (col. 2, lines 37-51).

VIII. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and Leibholz et al., US Patent No. 4,783,798 as applied to claim 12 above and further in view of Greenwood et al., US Pub. No. 2002/0033752.

As per claim 16:

Hellman et al. and Leibholz et al. substantially teach the method of claim 12. Not explicitly disclosed is the method wherein the transponder comprises a transceiver that sends and receives data using a 13.56 MHz radio frequency signal. However, Greenwood et al. teach that using 13.56MHz has benefits such as a lower power transmission and a greater range. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to send/receive data using a 13.56 MHz radio frequency signal. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Greenwood in paragraph 63.

IX. Claims 17 and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and further in view of Raspotnik, US Patent No. 5,832,090.

As per claim 17:

Hellman et al. substantially teach a device comprising: a processor and a transceiver (fig. 1, elements 15 and 31); a key generator operatively coupled to the transceiver and the processor (fig. 1, element 31); a communication interface to send and receive data from an external device via a communication link (fig. 1, element 19); and a memory coupled to the processor in which a plurality of machine instructions including an authenticated key agreement algorithm module are

stored that when executed by the processor performs the operations of: invoking the key generator to generate a key (fig. 1, element 21); passing a copy of the key to the transceiver (fig. 1, link between elements 21 and 31); enabling the transceiver to send a copy of the key to the external device to share the key between the device and the external device (fig. 1, elements 31, 19, and 32); and establishing a secure communication channel with the second device over the communication link that uses a cryptographic key that is generated through execution of the authenticated key agreement algorithm module in cooperative interaction with a symmetrical key agreement algorithm operating on the external device and is based on the key that is shared between the device and the external device (col. 4, line 1 – col. 5, line 3) .

Not explicitly disclosed is a transceiver to receive and send data via radio frequency RF signals. However, Raspotnik teaches transmitting/receiving data via radio frequency. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to transmit/receive the data via radio frequency signals. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Raspotnik in col. 2, lines 36-51.

As per claim 21:

Hellman et al. and Raspotnik substantially teach the device of claim 17. Furthermore, Raspotnik teaches the device further comprising a persistent memory device in which a device identifier is stored, and wherein execution of the machine instructions by the processor further performs the operation of sending data corresponding to the device identifier to the external device via the first RF signal (col. 2, line 37 - col. 3, line 17).

As per claim 22:

Hellman et al. substantially teach a device comprising: a processor and a transceiver to (fig. 1, elements 15 and 31); a communication interface to send data to and receive data from an external device via a communication link (fig. 1, element 19); and a memory coupled to the processor in which a plurality of machine instructions including an authenticated key agreement algorithm module are stored that when executed by the processor performs the operations of: controlling the transceiver to enable the transceiver to receive a copy of a shared key from the external device via a first signal (fig. 1, link between elements 21 and 31); and establishing a secure communication channel with the external device over the communication link, wherein the secure communication channel uses a cryptographic key that is generated through execution of the authenticated key agreement algorithm module through cooperative interaction with a symmetrical key agreement algorithm operating on the external device and is based on the shared key (col. 4, line 1 – col. 5, line 3).

Not explicitly disclosed is a transceiver to receive and send data via radio frequency RF signals. However, Raspotnik teaches transmitting/receiving data via radio frequency. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. to transmit/receive the data via radio frequency signals. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Raspotnik in col. 2, lines 36-51.

As per claim 23:

Hellman et al. and Raspotnik substantially teach the device of claim 22. Furthermore, Raspotnik teaches the device wherein the transceiver comprises a transponder reader to receive an RF signal generated by a compatible transponder that is operatively coupled to the external device (col. 2, lines 36-51).

As per claim 24:

Hellman et al. and Raspotnik substantially teach the device of claim 23. Furthermore, Raspotnik teaches the device further comprising an antenna coupled to the transponder reader and driven by the transponder reader to generate an RF signal including RF energy that is received by the compatible transponder to energize the compatible transponder (col. 2, lines 36-62).

X. Claims 18-20 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman et al., US Patent No. 4,200,770 and Raspotnik, US Patent No. 5,832,090 as applied to claims 17 and 22 above and further in view of Grube et al., US Patent No. 5,594,796.

As per claim 18:

Hellman et al. and Raspotnik substantially teach the device of claim 17. Furthermore, Raspotnik teaches the device wherein the transceiver comprises a transponder that transmits the first RF signal containing data corresponding to the copy of the key (col. 2, lines 37-51). Not explicitly disclosed is the device wherein the transponder transmits the first RF signal in response to receiving a second RF signal containing a data request from the external device.

However, Grube et al. teach that a user can request that a secure communication be established by requesting data which would invoke the transponder to transmit the data corresponding to the copy of the key. Therefore, it would have been obvious to a person in the

art at the time the invention was made to modify the method disclosed in Hellman et al. for the transponder transmits the first RF signal in response to receiving a second RF signal containing a data request from the external device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Grube et al., col. 1, lines 36-52.

As per claim 19:

Hellman et al. and Raspotnik substantially teach the device of claim 18. Furthermore, Raspotnik teaches the device wherein the transponder is energized to transmit the first RF signal by receiving RF energy via the second RF signal sent by the external device (col. 2, lines 36-62).

As per claim 20:

Hellman et al. and Raspotnik substantially teach the device of claim 17. Not explicitly disclosed is the device further comprising a user interface control, coupled to the processor, to receive a user request to establish a secure communication channel between the device and the external device. However, Grube et al. teach that a user can request that a secure communication be established by requesting data which would invoke the transponder to transmit the data corresponding to the copy of the key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. for a user interface control, coupled to the processor, to receive a user request to establish a secure communication channel between the device and the external device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Grube et al., col. 1, lines 36-

52.

As per claim 25:

Hellman et al. and Raspotnik substantially teach the device of claim 22. Not explicitly disclosed is the device further comprising a user interface control, coupled to the processor, to receive a user request to establish a secure communication channel between the device and the external device. However, Grube et al. teach that a user can request that a secure communication be established by requesting data which would invoke the transponder to transmit the data corresponding to the copy of the key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hellman et al. for a user interface control, coupled to the processor, to receive a user request to establish a secure communication channel between the device and the external device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Grube et al., col. 1, lines 36-52.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Nadia Khoshnoodi
Examiner
Art Unit 2133
8/15/2005

NK

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100